UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/789,808	02/27/2004	Michael D. Smith	418268002US	5627

45979 7590 07/23/2007

PERKINS COIE LLP/MSFT
P. O. BOX 1247
SEATTLE, WA 98111-1247

EXAMINER	
WANG, HARRIS C	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
07/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/789,808	SMITH ET AL.	
	Examiner	Art Unit	
	Harris C. Wang	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/14/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-43 are pending

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 5-7, 41-43 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 5 recites the limitation "when the codes provided by the service provider and the service consumer are not the same, attempting to derive the end code from the code provided by the service provider and when the attempt is successful, determining that the service provider has provided the requested service to the service consumer." Because the claim language was broad, the Examiner read the claims in light of the specifications to try to clarify the intentions of the claim.

Paragraph [0023] of the Applicant's specification teaches "when the service provider receives a request, it verifies that the code of the request can be used to derive the end code before providing the service." Therefore, receiving and verifying the end code does not prove that the provider provides the service, as it is a prerequisite for providing the service. In the case where the provider receives and verifies the end code, but does not provide the service (a legitimate cause for dispute) according to the claim language because the provider can give

the verified end code to the intermediary it is determined that "the service provider has provided the requested service to the service customer."

Claims 6-7 depend on Claim 5 and are rejected for the same rationale.

Claim 41 similarly recites the limitation "when the service provider provides a code from which the end code can be derived and the provided code supports the service provider's allegation of the services that were provided."

The Examiner rejects Claim 41 for the same reasons as Claim 5. Claims 42-43 depend on Claim 41 and are rejected for the same rationale as well.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 8-25, 29-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Briscoe (6341273).

Regarding Claims 1-2,

Briscoe teaches a method comprising:

registering with the service intermediary an indication of an end code of the service consumer wherein the indication of the end code is a start code from which the end code can be derived by the service intermediary.

("the user may be issued with the secret random number by a bank. This forms the beginning of the hash chain" Column 1, lines 63-64)

when the service consumer requests the service provider to provide a service, providing by the service consumer to the service provider a code derived from a start code using a function;

and when the service provider can verify that the end code can be derived from the code provided with a request, providing the requested service to the service consumer wherein the service provider can demonstrate to the service intermediary that it provided requested services to the service consumer when the code that was provided with a request can be used to derive the end code. *("The vendor validates this value by returning it to the issuing bank...The bank confirms to the vendor the validity of the value. Then if the user wants to transfer, for example, three units of value, it communicates to the vendor the hash value three steps back along the hash chain" Column 2, lines 8-16)*

The Examiner interprets the service intermediary as "the broker," the service customer as "the user" and the service provider as "the vendor."

While Briscoe does teach where the user provides the provider an end code Briscoe does not explicitly teach wherein the intermediary provides the end code to the service provider.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Briscoe to have the intermediary provide the end code to the service provider.

The motivation is that both the broker and user know the end code, so it makes no difference whether the broker or the user communicates the end code to the provider. One of ordinary skill would be able to send the end code from the intermediary rather than the user.

Regarding Claim 3,

Briscoe teaches the method of claim 1 wherein the registering include providing a start code and an end code. *("generating at the first party a first hash chain of values which are derived from the secret number by successive operations of a hash value" Column 2, lines 31-33) The Examiner interprets generating the codes at the broker as registering at the intermediary. The Examiner interprets the last hash on the end of the hash chain as the "end code."*

Regarding Claim 4,

Briscoe teaches the method of claim 1 wherein the service intermediary determines whether the end code can be derived from a code provided by a service provider by requesting the service consumer to provide the corresponding code and when the codes provided by the service provider and

the service consumer are the same, determining that the service provider has provided the requested services to the service consumer. *("The vendor communicates with the broker to verify the validity of the end-value derived form the value received from the client" Column 4, lines 62-64) The Examiner interprets the codes "are the same" as the verifying the validity of the end value derived from the value received from the client.*

Regarding Claim 8,

Briscoe teaches the method of claim 1. Briscoe does not explicitly teach wherein the service consumer requests the service provider to provide a service after the last requested service has been provided by the service provider.

Briscoe teaches a system "suitable for making the so-called "micropayments" required by low-value transactions. Generally, micropayment systems accumulate many micropayments, and collect the accumulated amount of money as one regular payment either before or after the transactions.

It would have been obvious to one of ordinary skill in the art to modify the system of Briscoe to request a service after the last requested service has been provided by the service provider.

The motivation is that micropayments are typically low values, sometimes less than a cent, so most of the micropayments occur one after another. One of

ordinary skill in the art would be able to request a service after the last requested service had been provided.

Regarding Claim 9,

Briscoe teaches the method of claim 1 wherein the service consumer can limit the number of outstanding requests for services to control exposure to liability for requested services that have not yet been provided. *("In all cases, vendor M1 has to be willing to relinquish their hold on the user's account (coin stick) by acknowledging they have received the message warning them not to accept further coins, before the bank can authorize another vendor to use the stick. Therefore, if the user wishes to have this flexibility, she must ensure the original contract with vendor M1 includes such an undertaking" Column 9, lines 19-25)*

Regarding Claims 10-11,

Briscoe teaches the method of claim 1 wherein the service consumer generates a sequence of codes using a function starting with the start code as input to the function *("generating at the second party ("the user") a second hash chain of values which are derived from the value communicated by the first party in step (d) (column 2, lines 31-33)")*wherein the service consumer provides the codes of the sequence to the service provider in reverse order of generation. *("to transfer a payment...the user communicates to the vendor the value at the end of the hash chain" Column 2, lines 4-8)*

Regarding Claim 12,

Briscoe teaches the method of claim 1 wherein the service provider verifies that the end code can be derived from a provided code by comparing a previously provided code to the result of applying a function to the provided code. *("The vendor validates this value by returning it to the issuing back. Using the hash function, the bank checks that the value is expected for the tenth hash value generated from the relevant random secret number." Column 2, lines 8-13)*

Regarding Claim 13,

Briscoe teaches the method of claim 1. Although Briscoe teaches that the consumer is issued a start code, Briscoe does not explicitly teach wherein the service consumer selects a start code.

It would have been obvious to one of ordinary skill in the art at the time of the invention to allow the consumer select the start code.

The motivation is that as long as both the intermediary and the consumer know the secret value, how the start code is delivered is not important. Therefore the Examiner considers the consumer selecting the start code an obvious modification.

Regarding Claim 14,

Briscoe teaches the method of claim 1 wherein the sequence of codes has a length. *("The payment module in the client first calculates the length n of the original coin stick" Column 6, lines 21-22)*

Regarding Claim 15,

Briscoe teaches the method of claim 14 wherein the length is agreed upon by the service provider and the service consumer. *("The transaction module in the vendor calculates the total price of the requested pages...and requests prepayment of this value from the client into its payment interface...The payment module in the client...it the calculates the number of iterations made unnecessary by the first payment" Column 6, lines 13-25) The Examiner interprets the agreed upon length as the number of micropayments necessary.*

Regarding Claim 16,

Briscoe teaches the method of claim 14 wherein the setting of the length of the sequence of codes can be used by the service provider to control exposure for liability for provided services for which payment has not yet been received.

Regarding Claim 17,

Briscoe teaches the method of claim 14 wherein the service intermediary provides the length to the service provider. *("The vendor connects to the broker's authorization interface...and requests confirmation that z is the value at the length of the coin stick with identity I issued to the client" Column 6, lines 33-37)*

Regarding Claims 18-19,

Briscoe teaches the method of claim 1. Briscoe does not explicitly teach wherein the service provider registers with the service intermediary an indication of an end code of the service provider and provides the service consumer with a code from which the end code of the service provider can be derived when a service is provided, wherein a code provided by the service provider to the service consumer can be used in determining whether the service consumer requested services.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the provider provide the end code and the code provided by the service provider can be derived when a service is provided.

The motivation is that the system of Briscoe essentially has three parties. By simply changing who sends the end code does not change the method of the system. One of ordinary skill would be able to have the provider provide the end code and send a code for each service requested.

Regarding Claim 20,

Briscoe teaches a method for requesting a service provider to provide services so that a service provider can demonstrate it provided services requested by a service consumer, the method comprising:

generating a sequence of codes that includes a start code and an end code using a one-way function; *("the user may be issued with the secret random number by a bank. This forms the beginning of the hash chain" Column 1, lines 63-64)*

registering with a service intermediary that the service consumer will request the service provider to provide services by providing a terminal code of the sequence and an identification of the service provider; *("The value at the end of the resulting has chain is communicated to the vendor" Column 6, lines 27-29)*

and for each service to be requested of the service provider, sending to the service provider a request for the service and a code of the sequence of codes in reverse order of generation so that the service provider can use that code to demonstrate that it provided a requested service. *("The vendor validates this value by returning it to the issuing bank...The bank confirms to the vendor the validity of the value. Then if the user wants to transfer, for example, three units of value, it communicates to the vendor the hash value three steps back along the hash chain" Column 2, lines 8-16)*

Regarding Claims 21-22,

Briscoe teaches the method of claim 20 wherein the service provider receives the end code from the service intermediary and when the service provider receives a request from a service consumer, it verifies whether the end code can be derived from the code of the request wherein the service provider provides the requested service only after it can be verified that the end code can be derived from the code of the request. *("The value at the end of the resulting has chain is communicated to the vendor" Column 6, lines 27-29) ("The vendor validates this value by returning it to the issuing bank...The bank confirms to the vendor the validity of the value. Then if the user wants to transfer, for example, three units of value, it communicates to the vendor the hash value three steps back along the hash chain" Column 2, lines 8-16)*

Regarding Claim 23,

Briscoe teaches the method of claim 21 wherein the service provider provides to the service intermediary a code provided in a service request *("The vendor validates this value by returning it to the issuing bank" Column 2, lines 8-16)*

Regarding Claim 24,

Briscoe teaches the method of claim 20 wherein the service intermediary stores the terminal code and provides the end code to service provider. *("A corresponding number n-p of hash values are repeatedly calculated, starting with the*

secret value...provided by the broker. The value...at the end of the resulting hash chain is communicated to the vendor" Column 2, lines 25-30)

Regarding Claim 25,

Briscoe teaches the method of claim 20 wherein when the service intermediary receives an indication that the service consumer disputes that the service provider provided the service that the service provider alleges it provided, resolving the dispute. *("If at any time the bank says the stick is valid, but the vendor tells the client it isn't, even though the broker has taken a coin off the stick, the client ahs redress because it can prove the broker said it was valid" Column 5, lines 5-10)*

Regarding Claims 26-28,

Briscoe teaches the method of claim 25. Briscoe does not explicitly teach wherein the service intermediary resolves the dispute in favor of the service provider when the service provider provides a code from which the end code can be derived and the provided code supports the service provider's allegation of the services that were requested, wherein the service intermediary determines whether the provided code can be used to derive the end code by comparing the provided code to a corresponding code provided by the service consumer, wherein the service intermediary determines whether the provided

code can be used to derive the end code by repeatedly applying the function to the provided code.

Asokan teaches a method where in the case of a dispute, attempting to derive the end code from the code provided by the service provider. *("In case of a dispute, R can submit the NRO (non-repudiation of origin) to an arbiter. The arbiter will verify...the token public key is in fact a hash of the alleged pre-image in the token." Pg. 5) The Examiner interprets R as a service provider.*

Asokan also teaches that "then the originator is allowed the opportunity to repudiate the token by...proving that S cheated by showing a different non-repudiation token corresponding to the same token public key."

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the dispute resolution method of Asokan with the method of Briscoe.

The motivation is that using hash chains in dispute resolution is well known in the art, and one of ordinary skill would be able to apply Asokans method with the teachings of Briscoe.

Regarding Claims 29-33,

Briscoe teaches a method for providing services requested by a service consumer so that a service provider can demonstrate it provided the requested services, the method comprising:

receiving from a service intermediary an indication that the service consumer has registered to request services of the service consumer and an end code; *("the user may be issued with the secret random number by a bank. This forms the beginning of the hash chain" Column 1, lines 63-64) ("The value at the end of the resulting has chain is communicated to the vendor" Column 6, lines 27-29)*

receiving requests for services from the service consumer, the requests including a code; when it can be determined that the end code can be derived from the code included from the request, providing the requested service; wherein the service provider determines whether the end code can be derived from a code included in a request by applying a function to the code included in the request, where it is inherent that a hash chain uses a one-way function. wherein a code generated by applying the function is compared to a code previously sent by the service consumer wherein the code previously sent is the last code received from the service consumer. *("for example, three units are required, then the payment module communicates to vendor the hash value which is three steps back in the hash chain from the current end value...The transaction module at the vendor receives this has value, checks that three further hashes result in the previous end hash value, if so stores the new end hash value in data store and supplies the goods" Column 6, lines 52-28)*

and providing to the service intermediary a code included in a request to demonstrate that the service provider provided requested services to the service consumer. *("The vendor validates this value by returning it to the issuing bank...The bank confirms to the vendor the validity of the value. Then if the user wants to transfer,*

for example, three units of value, it communicates to the vendor the hash value three steps back along the hash chain" Column 2, lines 8-16)

Regarding Claim 34,

Briscoe teaches a computer system for requesting a service provider to provide services, comprising:

a component that generates a sequence of codes that includes a start code and an end code using a one-way function; *("the coin stick issue module operates on this value z0 with a hash function to produce a hash value z1, operates on z1...to produce a further hash value z2 and so on. The processing with the hash function is iterated a predetermined number of times...and the resulting value zm is issued to the client" Column 5, lines 27-36)*

a component that registers with a service intermediary that a service consumer will request the service provider to provide services, the registering including providing to the service intermediary a terminal code of the sequence and an identification of the service provider; *("The transaction module in the vendor calculates the total price of the requested pages...and requests prepayment of this value from the client into its payment interface...The payment module in the client...it the calculates the number of iterations made unnecessary by the first payment" Column 13-25) The Examiner interprets the agreed upon length as the number of micropayments necessary.*

and a component that sends to the service provider requests for services and a code of the sequence of codes in reverse order of generation so that the

service provider can use the codes to demonstrate that the service consumer requested services. *("Subsequent requests for goods then require the pay numbe nodule to calculate the number of units of the coin stick denomination which are required to match the required price. For example, three units are required, then the payment module communicates to vendor the hash value which is three steps back in the hash chain from the current end value...The transaction module at the vendor receives this has value, checks that three further hashes result in the previous end hash value, if so stores the new end hash value in data store and supplies the goods" Column 6, lines 49-28)*

Regarding Claim 35,

Briscoe teaches the computer system of claim 34 wherein the codes are sent starting with the penultimate code of the sequence. *("The value z_{m+n-p} at the end of the resulting hash chain is communicated to the vendor" Column 6, lines 29-30)*

Regarding Claims 36-37,

Briscoe teaches the computer system of claim 34 wherein the service provider receives the end code from the service intermediary and when the service provider receives a request from a service consumer, it verifies whether the end code can be derived from the code of the request. wherein the service provider provides the requested service only after it can be verified that the end code can be derived from the code of the request. *("for example, three units are*

required, then the payment module communicates to vendor the hash value which is three steps back in the hash chain from the current end value...The transaction module at the vendor receives this has value, checks that three further hashes result in the previous end hash value, if so stores the new end hash value in data store and supplies the goods" Column 6, lines 52-28)

wherein the service provider provides to the service intermediary a code provided in a service request to demonstrate that the service consumer requested a service. *("The vendor validates this value by returning it to the issuing bank...The bank confirms to the vendor the validity of the value. Then if the user wants to transfer, for example, three units of value, it communicates to the vendor the hash value three steps back along the hash chain" Column 2, lines 8-16)*

Regarding Claim 39,

Briscoe teaches the computer system of claim 34 wherein the service intermediary stores the terminal code and provides an end code to service provider. *("the user may be issued with the secret random number by a bank. This forms the beginning of the hash chain" Column 1, lines 63-64) ("The value at the end of the resulting has chain is communicated to the vendor" Column 6, lines 27-29)*

Regarding Claim 40,

Briscoe teaches the computer system of claim 34 wherein when the service intermediary receives an indication that the service consumer disputes

that the service provider provided the service that the service provider alleges it provided, the service intermediary resolves the dispute. *("If at any time the bank says the stick is valid, but the vendor tells the client it isn't, even though the broker has taken a coin off the stick, the client ahs redress because it can prove the broker said it was valid" Column 5, lines 5-10)*

Claims 5-7, 26-28 and 41-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Briscoe in view of Asokan's Paper "Server-Supported Signatures" Published in the Journal of Computer Security in Fall 1997..

Regarding Claims 5,

Briscoe teaches the method of claim 4.

Briscoe does not explicitly teach when the codes provided by the service provider and the service consumer are not the same, attempting to derive the end code from the code provided by the service provider and when the attempt is successful, determining that the service provider has provided the requested service to the service consumer.

wherein when the attempt is unsuccessful attempting to derive the end code from the code provided by the service consumer and when the attempt to derive the end code from the code provided by the service consumer is successful, determining that the service provider has not provided the requested service to the service consumer.

Asokan teaches a method where in the case of a dispute, attempting to derive the end code from the code provided by the service provider. *("In case of a dispute, R can submit the NRO (non-repudiation of origin) to an arbiter. The arbiter will verify...the token public key is in fact a hash of the alleged pre-image in the token." Pg. 5) The Examiner interprets R as a service provider.*

Asokan also teaches that "then the originator is allowed the opportunity to repudiate the token by...proving that S cheated by showing a different non-repudiation token corresponding to the same token public key."

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the dispute resolution method of Asokan with the method of Briscoe.

The motivation is that using hash chains in dispute resolution is well known in the art, and one of ordinary skill would be able to apply Asokans method with the teachings of Briscoe.

Regarding Claim 7,

Briscoe and Asokan teach the method of Claim 6, it is inherent that when the attempt to derive the end code from the codes provided by the service consumer and service provider are unsuccessful that the codes provided by the server provider and the service consumer cannot be used to determine whether or not the service provider provided the requested services to the service consumer.

Regarding Claims 26-28,

Briscoe teaches the method of claim 25. Briscoe does not explicitly teach wherein the service intermediary resolves the dispute in favor of the service provider when the service provider provides a code from which the end code can be derived and the provided code supports the service provider's allegation of the services that were requested, wherein the service intermediary determines whether the provided code can be used to derive the end code by comparing the provided code to a corresponding code provided by the service consumer, wherein the service intermediary determines whether the provided code can be used to derive the end code by repeatedly applying the function to the provided code.

Asokan teaches a method where in the case of a dispute, attempting to derive the end code from the code provided by the service provider. *("In case of a dispute, R can submit the NRO (non-repudiation of origin) to an arbiter. The arbiter will verify...the token public key is in fact a hash of the alleged pre-image in the token." Pg. 5) The Examiner interprets R as a service provider.*

Asokan also teaches that "then the originator is allowed the opportunity to repudiate the token by...proving that S cheated by showing a different non-repudiation token corresponding to the same token public key."

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the dispute resolution method of Asokan with the method of Briscoe.

The motivation is that using hash chains in dispute resolution is well known in the art, and one of ordinary skill would be able to apply Asokans method with the teachings of Briscoe.

Regarding Claims 41-43,

Briscoe teaches the computer system of claim 40. Briscoe does not explicitly teach wherein the service intermediary resolves the dispute in favor of the service provider when the service provider provides a code from which the end code can be derived and the provided code supports the service provider's allegation of the services that were provided, wherein the service intermediary determines whether the provided code can be used to derive the end code by comparing the provided code to a corresponding code provided by the service consumer, wherein the service intermediary determines whether the provided code can be used to derive the end code by repeatedly applying the function to the provided code.

Asokan teaches a method where in the case of a dispute, attempting to derive the end code from the code provided by the service provider. *("In case of a dispute, R can submit the NRO (non-repudiation of origin) to an arbiter. The arbiter will*

verify...the token public key is in fact a hash of the alleged pre-image in the token." Pg. 5) The Examiner interprets R as a service provider.

Asokan also teaches that "then the originator is allowed the opportunity to repudiate the token by...proving that S cheated by showing a different non-repudiation token corresponding to the same token public key."

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the dispute resolution method of Asokan with the method of Briscoe.

The motivation is that using hash chains in dispute resolution is well known in the art, and one of ordinary skill would be able to apply Asokans method with the teachings of Briscoe.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Harris C. Wang whose telephone number is 5712701462. The examiner can normally be reached on M-F 8-5:30, Alternate Fridays Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ R. SHEIKH can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100